UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/259,620	02/26/1999	JAMES Q. MI	INTL-0160-US	5503

7590 10/08/2003

TIMOTHY N. TROP
TROP, PRUNER, HU & MILES
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/08/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 20

Application Number: 09/259,620
Filing Date: February 26, 1999
Appellant(s): MI ET AL.

Fred G, Pruner, Jr.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11 July 2003.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The amendment after final rejection filed on 09 July 2003 has been entered.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that independent claims 1, 6, 10, 15, 27, 31, and 35, with their dependent claims do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

5120939	Claus et al.	06-1992

5774544	Lee et al.	06-1998
5825884	Zdepski et al.	10-1998
6327578	Linehan	12-2001

Schneier, Bruce, Applied Cryptography, 2nd ed., 1996, pp. 53, 54, 185, and 186.

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1, 3, 6, 8, and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. (5120939) in view of Lee et al. (5774544).

Figure 1 of Claus et al. shows a second computer (element 500) receiving a request for identification (step 3) from a first computer (element 700). This meets the limitations of the first clause of the first claim. ID_n is retrieved from memory (550), anticipating retrieving a number that identifies the second computer system, and sent to the first computer. A cryptogram of ID_n (S_n) is further encrypted with a key shared with the first computer (see figure 2) by element 563. This covers encrypting the number with a key associated with the first computer system to produce a hash value. In step 4 the encrypted (or hashed) identifier is returned to the first computer, thereby showing the limitations of the last clause in claim 1. Element 720, which recreates the encryption done in the second computer, as opposed to decrypting the value received therefrom, shows that hashing is taught by Claus et al. S_n uniquely identifies the second computer because it is systematically derived from a value, ID_n, unique to element 500 (see lines 11-15 of column 5). A smart card is a computer because it comprises a processor and memory (see lines 33-34 of column 2). See also Claus et al.'s abstract. They do not

say that the unique identifier is a microprocessor number. In lines 12-23 of the first column, Lee et al. say that using serial numbers identifying microprocessors allows for better tracking of a hardware component. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor numbers, as taught by Lee et al., for the unique identifier in Claus et al. in order to improve control of Claus et al.'s smart cards.

The limitations of claim 3 are inherent; computer actions are done in response to the execution of instructions. Claim 6 is an apparatus for performing the steps of method claim 1 and is rejected for largely the same reasons. Claim 8 is inherent because instructions for the encryption and a unit to execute the instructions are necessary for the performance of the steps of the first claim. Lee et al. teaches a processor number that is a microprocessor number that uniquely identifies the second computer system.

2. Claims 4, 5, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Lee et al.

Claus et al. show a computer authenticating itself by supplying an encrypted version of a unique identifier to an authenticating computer. The only information shared by both the first and second computers is E_2, which includes a key. The origin of E_2 is vague, but generally it is said to have been programmed into the smart card during manufacture. The challenge number generator used in Claus et al. is capable of producing truly random numbers and can thus be used to generate encryption keys. With respect to claims 4 and 9, Claus et al. do not state that the key used to encrypt the

identifier is received from the authenticating computer. Official notice is taken that it is old and well-known to minimize the number of parties who have access to secret keys, such as those used in E_2 in Claus et al. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for the authenticating entity in Claus et al. to generate the key used in E_2 and send it to the smart card, thereby increasing security by keeping the parties privy to the key to a minimum.

With respect to claim 5, figure 6 in Claus et al. shows a networked environment, in which the two computers communicate via a public switched network. Communications over public networks render obvious web site addresses. As mentioned above, the only information that the two computers share is E_2. Claus et al. do not say that the key indicates an address of a web site. However, as the key (with its associated, generic algorithm) is the only shared piece of information, the web site address is necessarily indicated by the key. In other words, the one-to-one correspondence of the key to the host computer (element 600), mandates that the key is indicative of the web-site address.

3. Claims 10, 11, 13, 14, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zdepski et al. (5825884) in view of Schneier (*Applied Cryptography*) and Lee et al.

In lines 64-67 of column 4, Zdepski et al. talk about encrypting a platform's identifier with a recipient's public key. This renders obvious receiving the recipient's public key because use of the public key requires that it be present and thus have been

received. In the following column, this cryptogram is sent to the recipient. They do not say that any steps are taken to ensure that the public key is authentic or that the identifier uniquely identifies the platform. On pages 185-186, Schneier teaches certificates as a means to "thwart attempts to substitute one key for another". This is a type of verification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to verify the public key used in Zdepski et al. to avoid undesired key swaps as taught by Schneier.

In lines 12-23 of the first column, Lee et al. say that using serial numbers identifying microprocessors allows for better tracking of a hardware component. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor numbers, as taught by Lee et al., for the unique identifier in Zdepski et al. in order to improve control of Zdepski et al.'s platforms.

4. Claims 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, Zdepski et al., and Lee et al. as applied to claims 1 and 11 above, and further in view of Linehan (6327578).

Zdepski et al., Lee et al., and Schneier show sending identifiers encrypted with a recipient's verified public key. They do not say that the key indicates an URL address. In lines 14-20 of column 5, Linehan teaches including an URL in a certificate. Thus the public key would indicate an URL address. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to follow Linehan's example and include an URL address in the certificate of Schneier associated with the public key in Zdepski et al. This ties the key to a specific entity.

5. Claims 15, 16, 18-20, 27, 30, 31, 34, 35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Schneier.

Claus et al. show a computer authenticating itself by supplying an encrypted version of a unique identifier to an authenticating computer. They specifically teach encrypting with DES, but say, in lines 8-12 of column 8, that other enciphering computations could be used. They do not say that the encryption is a keyed hash. At the bottom of page 458, Schneier discloses keyed hashes with differing presumed security levels. In the simplest embodiment, the keyed hash is H(K, M). Keyed hashes curtail the ability of a malicious party to uncover the original K and M from the hash. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the keyed hashes taught by Schneier as the enciphering computation in Claus et al., thereby combating unwanted disclosure of the identifier and the key. As is apparent from the equation H(K, M), K and M are interchangeable. Thus, Claus et al.'s key is encrypted with the identifier, as per claim 15. For security reasons, the hash algorithm H would be assumed to be collision-resistant, non-commutative, and one-way.

6. Claims 17, 28, 32, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Schneier as applied to claim 15 above, and further in view of Lee et al.

Claus et al. and Schneier show a computer authenticating itself by supplying a key encrypted with an unique identifier to an authenticating computer. They do not say that the unique identifier is a microprocessor number. In lines 12-23 of the first column,

Lee et al. say that using serial numbers identifying microprocessors allows for better tracking of a hardware component. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor numbers, as taught by Lee et al., for the unique identifier in Claus et al. in order to improve control over Claus et al.'s smart cards.

7. Claims 29, 33, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Schneier as applied to claims 27, 31, and 35 above, and further in view of Linehan.

Claus et al. and Schneier show a computer authenticating itself by supplying a key encrypted with an unique identifier to an authenticating computer. They do not say that the key indicates an URL address. In lines 14-20 of column 5, Linehan teaches including an URL in a certificate, which can be used to authenticate a key. Thus the key indicates an URL address. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to follow Linehan's example and include an URL address in a certificate associated with the key in Claus et al. This ties the key to a specific entity.

(11) Response to Argument

A. With respect to claim 1, applicant argues that Claus et al. show identification of a user of a smart card, not identification of the processor of the smart card. The identifier in question is a PIN (line 35 of column 4). PINs are pieces of information that should only be known by the user. As such, applicant's idea that Claus et al. show the identification of a user is basically logical. However, a PIN is used, generally, with a

card. As such, the PIN also identifies that card. Claus et al. specifically recognize this fact in lines 11-13 of column 5, saying that the PIN "is unique to that card." This teaching is the crux of the rejection because it shows that the identifier uniquely identifies the smart card. Applicant has regrettably declined from any direct comments about the applicability of this teaching.

As applicant notes, Lee et al. ('544) teaches that the card's unique number should be a microprocessor number. Applicant opines that the examiner has not provided support for the motivation to combine Lee et al. with Claus et al. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner cited lines 12-23 of column 1. This section specifically says that "[a]ddition of a serial number allows a manufacturer to trace a product in the field back to the original equipment manufacturer [and] allows the manufacturer greater control over its product." The motivation to combine is the greater control gained by the manufacturer. Thus, the examiner has clearly presented "language from a prior art reference showing the alleged suggestion or motivation."

Applicant ends the analysis of the rejection of claim 1 with a discussion of the system that would result from the examiner's proposed combination of Claus et al. and Lee et al. Applicant is of the opinion that replacing the PIN with a processor number would make Claus et al.'s system unsatisfactory for its intended purpose. This line of reason is flawed on many levels, the first of which is that the processor number is "replacing" the PIN. Claus et al. is largely silent with respect to the constitution of the PIN. The only certainty is that it uniquely identifies the card. As such, the PIN and the processor number are not mutually exclusive; correctly speaking, the processor number is *used as* the PIN in the combination of the references.

To continue, applicant limits his understanding PIN numbers to numbers that identify. As mentioned above, this is technically correct, but it misses nuances that are inseparable from the practices involved with PINs. Let us use the examiner's freshman extension, 6669, in an example. By itself, 6669, despite being a PIN, does not identify anyone. It does not, by itself, identify an user. It only identifies an user when it is presented by an entity and compared with a number that is stored and associated with the user's identity. If the number presented by the entity and the stored number match, the user is assumed to be the user stored in the database. The combination of Claus et al. and Lee et al. uses the processor number as the PIN. Thus the processor number identifies a presenting entity while at the same time uniquely identifying the processor. The intent of Claus et al. is thus maintained while the limitations of the claims are met.

B. Applicant's arguments with respect to claims 6, 8, 9, 23 and 24 are largely the same as those presented with respect to claim 1. They are unpersuasive for the same reasons.

C. With respect to claim 10 and its dependents, applicant notes that the examiner has not cited language that teaches selectively authorizing encryption based on identification of another processor-based system. The examiner has cited pages 185-186 of Schneier which teach the use of digital certificates. Digital certificates are used to ensure that keys belong to the entities that claim to own the keys. As such they are used in identification. While not explicitly discussed in the rejection, a person of ordinary skill in the art understands that, if the identification fails – that is, the entity claiming to own the key is not identified as the entity that owns the key, encryption using the key would not be enacted; encryption would be, selectively, de-authorized. As such, the limitations of claim 10, and its dependents, are met.

D. Applicant brings up several limitations in claim 15 that are alleged to be absent from the rejection. The instruction unit is not explicitly mentioned in the rejection, although, given its breadth, any piece of hardware that receives data and is in communication with a processor performing encryption reads on this feature. Elements 563 or 561 in Claus et al.'s first figure would both work. An input port, which is inherent to Claus et al.'s smartcard, also meets this limitation. Applicant also is of the opinion that the rejection does not show the furnishing of a hash value to external pins of a processor. The hash value in Claus et al. is sent to a different entity, which inherently

entails the hash traveling to external pins of a processor. Thus applicant's arguments with respect to claim 15 and its dependents are unpersuasive.

E. With respect to claims 27-30, Claus et al.'s authentication device or first computer system stores information, as noted throughout their disclosure (for example, lines 61-62 of column 1 and lines 33-37 of column 3). This information reads on applicant's database. The hash value gives access to this information, thereby identifying it, albeit indirectly. Claims 27-30 are hence rendered obvious.

F. Claims 31-34 are rejected for largely the same reasons as claims 27-30, with applicant making largely the same arguments. Applicant's arguments with respect to claims 31-34 are unpersuasive for largely the same reasons as the arguments with respect to claims 27-30.

G. Claims 35-38 are rejected for largely the same reasons as claims 27-30 or 31-34, with applicant making largely the same arguments. Applicant's arguments with respect to claims 35-38 are unpersuasive for largely the same reasons as the arguments with respect to claims 27-30 or 31-34.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
October 5, 2003

Conferees
Gilberto Barrón
Matthew Smithers

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TIMOTHY N. TROP
TROP, PRUNER, HU & MILES
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137